

# **F-Secure Anti-Virus 2013**



# indekiler

<b>Bölüm 1: Yükleme.....</b>	<b>5</b>
İlk kez yüklemeden önce.....	6
Ürünü ilk kez yükleme.....	6
Uygulamaları yükleme ve yükseltme.....	6
Yardım ve Destek.....	7
 <b>Bölüm 2: Bakarken.....</b>	 <b>9</b>
Otomatik güncelle tirmeler nasıl kullanılır.....	10
Güncelle tirme durumunu denetleme.....	10
İnternet bağlantı ayarlarınızı denetleme.....	10
Gerçek Zamanlı Koruma A ının durumunu denetleme.....	11
Ürünün neler yaptığını görme.....	11
Bildirim geçmişi görüntüle.....	11
Bildirim ayarlarını denetleme.....	11
Gerçek Zamanlı Koruma A ı.....	12
Gerçek Zamanlı Koruma A ı nedir?.....	12
Gerçek Zamanlı Koruma A ının faydaları.....	12
Hangi verilere katkıda bulunursunuz?.....	13
Gizliliğiniz nasıl korunuyor?.....	14
Gerçek Zamanlı Koruma A ı katılımcısı olma.....	14
Gerçek Zamanlı Koruma A ı ile ilgili sorular.....	14
Aboneli imin geçerli olduğunu nasıl bilebilirim.....	15
Eylem merkezi.....	15
Aboneli i etkinleştir.....	15
 <b>Bölüm 3: Giriş .....</b>	 <b>17</b>
Genel koruma durumunuzu görüntüleme.....	18
Ürün istatistiklerini görüntüleme.....	18
Ürün güncelle tirmelerini izleme.....	19
Veritabanı sürümlerini görüntüleme.....	19
Cep telefonu geniş bant ayarlarınızı denetleme.....	19
Virüsler ve diğer kötü amaçlı yazılımlar nedir.....	20
Virüsler.....	20
Casus yazılımlar.....	20
Kendini gizleyen yazılımlar.....	21
Riskli yazılımlar.....	21

## **Bölüm 4: Kötü amaçlı yazılımlara karşı bilgisayarınızı koruma.....23**

Bilgisayarınızı nasıl tarayabilirim.....	24
Dosyaları otomatik olarak tarama.....	24
Dosyaları elle tarama.....	26
E-postaları tarama.....	29
Tarama sonuçlarını görüntüleme.....	29
Dosyalar nasıl taramanın dışında bırakılır.....	30
Dosya türlerini dışlama.....	30
Konuma göre dosyaları dışlama.....	31
Dışlanan uygulamaları görüntüleme.....	31
Karantina nasıl kullanılır.....	32
Karantinaya alınan öğeleri görüntüleyin.....	32
Karantinaya alınan öğeleri geri yükleme.....	33
DeepGuard nedir.....	33
DeepGuard'ı açma veya kapatma.....	33
DeepGuard'ın engellediği uygulamalara izin verme.....	34
DeepGuard'ı uyumluluk modunda kullanma.....	34
Üşheli davranış uyarılarıyla ne yapmak gerekir.....	34

## Yükleme

---

### Konular:

- *İlk kez yüklemekten önce*
- *Ürünü ilk kez yükleme*
- *Uygulamaları yükleme ve yükseltme*
- *Yardım ve Destek*


## İlk kez yüklemeden önce

F-Secure ürününü seçtiğiniz için teşekkür ederiz.

Ürünü yükleyebilmek için şunlara ihtiyacınız vardır:

- Yükleme CD'si veya yükleme paketi. CD sürücüsü olmayan bir netbook kullanıyorsanız, yükleme paketini [www.f-secure.com/netbook](http://www.f-secure.com/netbook) adresinden yükleyebilirsiniz.
- Abonelik anahtarınız.
- İnternet bağlantısı.

Başka bir üreticiye ait bir güvenlik ürününüz varsa, yükleyici onu otomatik olarak kaldırmaya çalışacaktır. Bu gerçekle karşılaşmazsanız, lütfen el ile kaldırın.

 **Not:** Bilgisayarda birden fazla hesabınız varsa, yükleme işlemi için yönetici ayrıcalıklarıyla oturum açın.

## Ürünü ilk kez yükleme

Ürünü yükleme yönergeleri

Ürünü yüklemek için şu yönergeleri uygulayın:

1. CD'yi yerle tirin veya indirdiğiniz yükleyiciyi çift tıklayın.  
CD otomatik olarak bağlanmazsa Windows Gezgini'ne gidin, CD-ROM simgesini ve yüklemeyi başlatmak için de yükleme dosyasını çift tıklayın.
2. Ekrandaki yönergeleri uygulayın.
  - Ürünü bir mağazadan CD olarak satın aldıysanız, abonelik anahtarını Hızlı Yükleme Kılavuzu kapağında bulabilirsiniz.
  - Ürünü F-Secure eStore'dan yüklediyseniz, abonelik anahtarı satın alma siparişinin onay e-postasında bulunur.

Aboneliğinizi doğrulamadan ve İnternet'ten en son güncellemeleri yüklemeden önce bilgisayarınızın yeniden bağlanması gerekebilir. CD'den yüklüyorsanız, bilgisayarınızı yeniden bağlatmadan önce Yükleme CD'sini çıkarmayı unutmayın.

## Uygulamaları yükleme ve yükseltme

Yeni aboneliğinizi etkinleştirme yönergeleri.

Yeni aboneliğinizi etkinleştirmek veya başlatma ekranını kullanarak yeni bir uygulama yüklemek için şu yönergeleri uygulayın:

 **Not:** Başlatma ekranı simgesini Windows sistem tepesinde bulabilirsiniz.

1. Başlatma panelinde en sağdaki simgeyi seçin.  
Bir açılır menü ekrana gelir.
2. **Aboneliklerimi görüntüle**'yi seçin
3. **Aboneliklerim** altında, **Abonelik durumu** sayfasına gidin ve **Aboneliğinizi etkinleştir**'i tıklayın.  
**Aboneliğinizi etkinleştir** penceresi açılır.
4. Uygulama için abonelik anahtarınızı girin ve **Tamam**'ı tıklayın.

5. Aboneli iniz do rulandıktan ve etkinle tirildikten sonra, **Kapat**'ı tıkladın.
6. **Aboneliklerim** altında, **Y¼kleme durumu** sayfasına gidin. Y¼kleme otomatik olarak ba latılmazsa, u yönergeleri uygulayın:
  - a) **Y¼kle**'yi tıkladın.  
Y¼kleme penceresi açılır.
  - b) **İeri**'yi tıkladın.  
Uygulama indirilir ve y¼kleme i lemi ba lar.
  - c) Y¼kleme tamamlandı ında, **Kapat**'ı tıkladın.

Yeni abonelik etkinle tirilmi tir.

## Yardıı ve Destek

---

¼rün ekranında herhangi bir yerde Yardıı simgesini tıklatarak veya F1'e basarak çevrimiçi olarak ¼rün yardıına eri ebilirsiniz.

Lisansınızı kaydettikten sonra, ¼cretsiz ¼rün g¼ncellemeleri ve ¼rün deste i gibi ek hizmetler almaya hak kazanırsınız. [www.f-secure.com/register](http://www.f-secure.com/register) adresinden kaydolabilirsiniz.





## Ba larken

---

### Konular:

- *Otomatik güncelle tirmeler nasıl kullanılır*
- *Ürünün neler yaptı ını görme*
- *Gerçek Zamanlı Koruma A ı*
- *Aboneli imin geçerli oldu unu nasıl bilebilirim*

Ürünü kullanmaya nasıl ba layaca ınız ile ilgili bilgiler.

Bu bölümde, ba latma paneli aracılı ıyla ortak ayarların nasıl de i tirilece i ve aboneliklerinizin nasıl yönetilece i açıklanır.

Ba latma panelinin ortak ayarları, ba latma panelinde yüklü olan tüm programlara uygulanan ayarlardır. Bu ayarları her bir program için ayrı ayrı de i tirmek yerine, yüklü olan tüm programlar tarafından kullanılan ortak ayarları düzenlemeniz yeterlidir.

Ba latma panelindeki ortak ayarlar unlardır:

- Kar ıdan Yüklemler altından, kar ıdan yüklenmi güncelle tirmeler ile ilgili bilgileri görüntüleyebilir ve yeni güncelle tirmeler olup olmadı ını el ile denetleyebilirsiniz.
- Ba lanma ayarları altından, bilgisayarınızın Internet'e ba lanma biçimini de i tirebilirsiniz.
- Bildirimler altından, geçmi bildirimleri görüntüleyebilir ve hangi bildirim türlerini görmek istedi inizi ayarlayabilirsiniz.
- Gizlilik ayarları altından, bilgisayarınızın Gerçek Zamanlı Koruma A ı'na ba lanmasına izin verilip verilmedi ini seçebilirsiniz.

Yüklü programlar için aboneliklerinizi de ba latma paneli aracılı ıyla yönetebilirsiniz.

## Otomatik gncelle tirmeler nasıl kullanılır

Otomatik gncelle tirmeler bilgisayarınızın korumasını gncel tutar.

rn, Internet'e ba lı oldu unuzda en yeni gncelle tirmeleri bilgisayarınıza alır. A trafi ini algılar ve yava bir a ba lantısında bile di er Internet trafi ini rahatsız etmez.

### Gncelle tirme durumunu denetleme


Son gncelle tirme tarih ve saatini grntleyin.

Otomatik gncelle tirmeler aık oldu unda, Internet'e ba lı oldu unuzda rn en son gncelle tirmeleri otomatik olarak alır.

Elinizde en yeni gncelle tirmelerin bulundu undan emin olmak iin:

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.  
Aılır men grntlenir.
2. **Ortak ayarları a** seene ini belirtin.
3. **Otomatik gncelle tirmeler** > **Kar ıdan yklemeler**'i sein.
4. **imdi denetle**'yi tıklatın.

rn Internet'e ba lanır ve en son gncelle tirmeleri denetler. Koruma gncel de ilse, en yeni gncelle tirmeleri alır.

 **Not:** Internet'e ba lanmak iin modem kullanıyorsanız veya ISDN ba lantınız varsa, gncelle tirmeleri denetleyebilmek iin ba lantının etkin olması gerekir.


### Internet ba lantı ayarlarınızı de i tirme

Genelde varsayılan ayarların de i tirilmesi gerekmez, ancak gncelle tirmeleri otomatik olarak alabilmeniz iin sunucunun Internet'e ba lanma biimini yapılandırabilirsiniz.


Internet ba lantı ayarlarınızı de i tirmek iin:

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.  
Aılır men grntlenir.
2. **Ortak ayarları a** seene ini belirtin.
3. **Otomatik gncelle tirmeler** > **Ba lantı**'yı sein.
4. **Internet ba lantısı** listesinde, bilgisayarınızın Internet'e nasıl ba landı ını sein.

- Kalıcı bir a ba lantınız varsa **Her zaman ba lı varsay** seene ini belirleyin.

 **Not:** Bilgisayarınızın kalıcı bir a ba lantısı yoksa ve istendi inde ba lanmak zere ayarlanmı sa, **Her zaman ba lı varsay** seene ini belirlemek birden fazla evirmeli ba lantıya neden olabilir.

- Yalnızca rn tarafından etkin bir a ba lantısı algılandı ında gncelle tirmeleri almak iin **Ba lantıyı algıla** seene ini belirleyin.
- Yalnızca rn tarafından ba ka a trafi i algılandı ında gncelle tirmeleri almak iin **Trafi i algıla** seene ini belirleyin.

 **pucu:** Etkin a ba lantısı olmasa da **Ba lantıyı algıla** ayarının etkin bir a ba lantısı algılamasına neden olan sıra dı ı bir donanım yapılandırmanız varsa, bunun yerine **Trafi i algıla**'yı sein.

5. **HTTP proxy** listesinde, bilgisayarınızın Internet'e ba lanmak iin *proxy sunucu* kullanıp kullanmadı ını belirleyin.

- Bilgisayarınız Internet'e do rudan ba lanıyorsa, **HTTP proxy yok'u** seçin.
- **HTTP proxy'yi elle yapılandır** ö esini seçerek **HTTP proxy** ayarlarını yapılandırın.
- Web tarayıcınızda yapılandırdı ınız **HTTP proxy** ayarlarını kullanmak için **Tarayıcının HTTP proxy'sini kullan** seçene ini belirleyin.

## Gerçek Zamanlı Koruma A ı'nın durumunu denetleme

Ürünün birçok özelli inin düzgün çalı ması için Gerçek Zamanlı Koruma A ı'na ba lantı gerekir.

A sorunları varsa veya güvenlik duvarınız Gerçek Zamanlı Koruma A ı trafi ini engelliyorsa, durum 'ba lı de il' olarak görünür. Gerçek Zamanlı Koruma A ı'na eri im gerektiren herhangi bir ürün özelli i yüklü de ilse, durum 'kullanılmıyor' olarak görünür.

Durumu denetlemek için:

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.  
Açılır menü görüntülenir.
2. **Ortak ayarları aç** seçene ini belirtin.
3. **Otomatik güncelle tirmeler > Ba lantı'yı** seçin.

**Gerçek Zamanlı Koruma A ı** altında, Gerçek Zamanlı Koruma A ı'nın geçerli durumunu görebilirsiniz.

## Ürünün neler yaptı ını görme

Ürünün bilgisayarınızda gerçekle tirdi i eylemleri **Bildirimler** sayfasından görebilirsiniz.

Ürün bir eylem gerçekle tirdi inde, örne in bir virüs bulup engelledi inde bir bildirim görüntüler. Bazı bildirimler, örne in kullanılabilir yeni hizmetler konusunda bilgilendirilmeniz için servis sa layıcınız tarafından da gönderilebilir.

## Bildirim geçmi ini görüntüle

Görüntülenmi olan bildirimleri, bildirim geçmi inde görebilirsiniz

Bildirim geçmi ini görüntülemek için:

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.  
Açılır menü görüntülenir.
2. **Ortak ayarları aç** seçene ini belirtin.
3. **Di er > Bildirimler'i** seçin.
4. **Bildirim geçmi ini göster'i** tıklatın.  
Bildirim geçmi i listesi açılır.

## Bildirim ayarlarını de i tirme

Ürünün hangi bildirim türlerini görüntülemesini istedi inizi seçebilirsiniz.

Bildirim ayarlarını de i tirmek için:

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.  
Açılır menü görüntülenir.
2. **Ortak ayarları aç** seçene ini belirtin.
3. **Di er > Bildirimler'i** seçin.

4. Program iletilerini etkinle tirmek veya devre dı ı bırakmak için **Program iletilerine izin ver**'i seçin veya seçimini kaldırın.  
Bu ayar etkinle tirildi inde, ürün, yüklü programların bildirimlerini görüntüler.
5. Tanıtım iletilerini etkinle tirmek veya devre dı ı bırakmak için **Tanıtım iletilerine izin ver**'i seçin veya seçimini kaldırın.
6. **Tamam**'ı tıklatın.

## Gerçek Zamanlı Koruma A ı

Bu belgede, F-Secure Corporation tarafından sa lanan ve temiz uygulamaları ve web sitelerini tanımlamanın yanı sıra kötü amaçlı yazılımlara ve web sitesi yararlanmalarına kar ı koruma sa layan bir çevrimiçi hizmet olan Gerçek Zamanlı Koruma A ı açıklanır.

## Gerçek Zamanlı Koruma A ı nedir?

Gerçek Zamanlı Koruma A ı, Internet tabanlı en son tehditlere hızlı yanıt verilebilmesini sa layan bir çevrimiçi hizmettir.

Gerçek Zamanlı Koruma A ı katılımcısı olarak yeni ortaya çıkan tehditlere kar ı korumayı güçlendirmemize yardımcı olabilirsiniz. Gerçek Zamanlı Koruma A ı, belli ba ılı bilinmeyen, kötü amaçlı veya üpheli uygulamaların ve bu uygulamaların aygıtınızda yaptıklarının istatistiklerini toplar. Bu bilgiler anonimdir ve veri analiziyle birle tirilmek üzere F-Secure Corporation'a gönderilir. Analiz edilen bilgileri, en son tehditlere ve kötü amaçlı yazılımlara kar ı aygıtınızdaki güvenli i artırmak için kullanırız.

## Gerçek Zamanlı Koruma A ı nasıl çalışıyor?

Gerçek Zamanlı Koruma A ı katılımcısı olarak, bilinmeyen uygulamalar ve web siteleri ile web sitelerindeki kötü amaçlı uygulamalar ve güvenlik açıkları hakkında bilgi sa layabilirsiniz. Gerçek Zamanlı Koruma A ı web'deki etkinli ini izlemeyebilir veya zaten analiz edilmi olan web siteleriyle ve bilgisayarınıza yüklü temiz uygulamalarla ilgili bilgi toplamaz.

Bu verilere katkıda bulunmak istemiyorsanız, Gerçek Zamanlı Koruma A ı yüklü uygulamalar veya ziyaret edilen web siteleriyle ilgili bilgi toplamaz. Ancak ürün, uygulamaların, web sitelerinin, iletilerin ve di er nesnelerin geçmi i açısından F-Secure sunucularını sorgulamak zorundadır. Sorgulama ifreli bir sa lama toplamı kullanılarak yapıldı ından sorgulanan nesnenin kendisi F-Secure'a gönderilmez. Kullanıcılara ili kin verileri izlemeyiz; yalnızca dosyanın veya web sitesinin isabet sayacı artırılır.

Gerçek Zamanlı Koruma A ı ile ilgili a trafi i tümüyle durdurulamaz, çünkü ürün tarafından sa lanan korumanın ayrılmaz bir parçasıdır.

## Gerçek Zamanlı Koruma A ı'nın faydaları

Gerçek Zamanlı Koruma A ı ile en son tehditlere kar ı daha hızlı ve daha do ru korumaya sahip olacak, kötü amaçlı olmayan üpheli uygulamalar için gereksiz uyarılar almayacaksınız.

Gerçek Zamanlı Koruma A ı katılımcısı olarak yeni ve algılanmamı kötü amaçlı yazılımları bulmamıza ve virüs tanımı veritabanımızdan hatalı pozitif sonuçları kaldırmamıza yardımcı olabilirsiniz.

Gerçek Zamanlı Koruma A ı'ndaki tüm katılımcılar birbirine yardım eder. Gerçek Zamanlı Koruma A ı aygıtınızda üpheli bir uygulama buldu unda, aynı uygulamanın daha önce ba ka aygıtlarda bulundu unda elde edilen çözümleme sonuçlarından yararlanabilirsiniz. Gerçek Zamanlı Koruma A ı, aygıtınızın genel performansını artırır; çünkü yüklü güvenlik ürününün Gerçek Zamanlı Koruma A ı tarafından daha önce çözümlenmi ve temiz oldu u belirlenmi uygulamaları yeniden taraması gerekmez. Benzer ekilde, kötü amaçlı web siteleri ve istenmeyen toplu iletiler ile ilgili bilgiler de Gerçek Zamanlı Koruma A ı aracılı ıyla payla ılır; böylece, web sitesinden yararlanma giri imlerine ve istenmeyen posta iletilerine kar ı daha do ru bir koruma sa lanabilir.

Gerçek Zamanlı Koruma A ı'na ne kadar çok insan katkıda bulunursa, tek tek katılımcılar da o oranda daha iyi korunur.

## Hangi verilere katkıda bulunursunuz?

Gerçek Zamanlı Koruma A ı katılımcısı olarak aygıtınızdaki uygulamalar ve ziyaret etti iniz web siteleri ile ilgili bilgi sa larsınız; böylece Gerçek Zamanlı Koruma A ı en yeni kötü amaçlı uygulamalar ve üpheli web sitelerine kar ı korunmanızı sa layabilir.

### Dosya yorumunu çözümleme

Gerçek Zamanlı Koruma A ı yalnızca bilinen bir yorum bulunmayan uygulamalar ve üpheli ya da kötü amaçlı oldu u bilinen dosyalar ile ilgili bilgileri toplar.

Gerçek Zamanlı Koruma A ı yalnızca Ta ınabilir yürütülebilir dosyalar (Windows platformundaki .cpl, .exe, .dll, .ocx, .sys, .scr ve .drv dosya uzantılı Ta ınabilir Yürütülebilir dosyalar gibi) ile ilgili bilgileri toplar.

Toplanan bilgiler unları içerir:

- uygulamanın aygıtınızda bulundu u dosya yolu,
- dosyanın boyutu ve olu turulma ya da de i tirilme tarihi,
- dosya öznitelikleri ve ayrıcalıklar,
- dosya imzası bilgileri,
- dosyanın geçerli sürümü ve dosyayı olu turan irket,
- dosyanın kayna ı veya kar ıdan yükleme URL'si,
- taranan dosyaların F-Secure DeepGuard ve virüsten koruma çözümlemesi sonuçlarını
- di er benzer bilgiler.

Gerçek Zamanlı Koruma A ı, etkilenmi oldukları belirlenmedikçe ki isel belgelerinizle ilgili herhangi bir bilgi toplamaz. Kötü amaçlı dosya türleri için, etkilenmenin adı ve dosyanın temizleme durumu ile ilgili bilgiler toplanır.

Gerçek Zamanlı Koruma A ı aracılı ıyla, çözümlenmek üzere üpheli yazılımları da gönderebilirsiniz. Gönderebilece iniz uygulamalar yalnızca Ta ınabilir Yürütülebilir dosyalar olabilir. Gerçek Zamanlı Koruma A ı hiçbir zaman ki isel belgelerinizle ilgili herhangi bir bilgi toplamaz ve bu tür dosyalar hiçbir zaman çözümlenmek üzere otomatik olarak kar ıya yüklenmez.

### Dosyaları çözümlenmek üzere gönderme

Gerçek Zamanlı Koruma A ı ile üpheli uygulamaları analiz için göndermeniz de mümkündür.


Üpheli uygulamaları, ürün sizden bunu istedi i zaman gönderebilirsiniz. Yalnızca Ta ınabilir Yürütülebilir dosyaları gönderebilirsiniz. Gerçek Zamanlı Koruma A ı hiçbir zaman ki isel belgelerinizi yüklemez.

### Web sitesi yorumunu çözümleme

Gerçek Zamanlı Koruma A ı, web etkinli inizi izlemez veya daha önce çözümlenmi olan web siteleri ile ilgili bilgi toplamaz. Web'de gezindi iniz sırada ziyaret etti iniz web sitelerinin güvenli oldu undan emin olmanızı sa lar. Bir web sitesini ziyaret etti inizde, Gerçek Zamanlı Koruma A ı bu sitenin güvenilir olup olmadı ını denetler ve site üpheli ya da zararlı olarak derecelendirilmi se size bildirir.

Ziyaret etti iniz web sitesinde kötü amaçlı veya üpheli içerik varsa veya bilinmeyen bir yararlanma kodu kullanılıyorsa, Gerçek Zamanlı Koruma A ı, web sayfası içeri inin çözümlenebilmesi için bu sitenin tüm URL'sini toplar.

Henüz derecelendirilmemi bir siteyi ziyaret ederseniz, Gerçek Zamanlı Koruma A ı, sitenin çözümlenebilmesi ve derecelendirilebilmesi için etki alanı ve alt etki alanı adlarının yanı sıra bazı durumlarda ziyaret edilen sayfanın yolunu da toplar. Gizlili inizi korumak için, ki isel olarak tanımlanmanıza olanak verebilecek ekilde sizinle ba lantılı olan bilgiler içerebilecek tüm URL parametreleri kaldırılır.

 **Not:** Gerçek Zamanlı Koruma A ı özel a lardaki web sayfalarını derecelendirmez veya çözümlemez; bu nedenle de özel IP a ı adreslerinden (örne in, kurumsal intranetlerden) hiçbir bilgi toplamaz.

### Sistem bilgisini çözümleme

Gerçek Zamanlı Koruma A ı, hizmeti izleyebilmemiz ve geli tirebilmemiz için i letim sisteminizin adı ve sürümü, Internet ba lantısı ve Gerçek Zamanlı Koruma A ı kullanım istatistikleri (örne in, web sitesi yorumunun sorgulanma sayısı ve sorgunun bir sonuç döndürmesi için geçen ortalama süre) ile ilgili bilgi toplar.

## Gizlili iniz nasıl korunuyor?

Bu bilgileri güvenli ekilde aktarır ve verilerin içerebilece i ki isel bilgileri otomatik olarak kaldırırız.

Gerçek Zamanlı Koruma A ı, kimlik belirleyici verileri F-Secure'a göndermeden önce kaldırır ve aktarım sırasında toplanan tüm bilgileri ifreleyerek yetkisiz eri imden korunmasını sa lar. Toplanan bilgiler tek tek i lenmez; di er Gerçek Zamanlı Koruma A ı katılımcılarından alınan bilgilerle birlikte gruplandırılır. Tüm veriler istatistiksel ve anonim olarak analiz edilir; bu, hiçbir verinin hiçbir ekilde size ba lanmayaca ı anlamına gelir.

Toplanan veriler, sizi ki isel olarak tanımlayabilecek herhangi bir bilgi içermez. Gerçek Zamanlı Koruma A ı özel IP adresini ya da e-posta adresleri, kullanıcı adları ve parolalar gibi di er özel bilgileri toplamaz. Ki isel olarak tanımlanmanıza yol açabilecek tüm verileri kaldırmaya çalı mamıza kar ın, toplanan bilgilerde bu tür veriler kalabilir. Bu gibi durumlarda, istenmeden toplanan verileri sizi ki isel olarak tanımlamak için kullanmayaca ız.

Toplanan bilgilerin aktarılması, depolanması ve i lenmesi sırasında katı güvenlik önlemleri ve fiziksel, yönetsel ve teknik korumalar uygularız. Bu bilgiler, kendi ofislerimizde veya alt yüklenicilerimizin ofislerinde bulunan güvenli konumlarda ve bizim denetimimizdeki sunucularda depolanır. Toplanan bilgilere yalnızca yetkili personel eri im sa layabilir.

F-Secure toplanan verileri ba lı irketleri, alt yüklenicileri, da ıtımcıları ve ortaklarıyla payla abilir; ancak bunu her zaman, ki isel olarak tanımlanamayacak anonim bir biçimde yapar.

## Gerçek Zamanlı Koruma A ı katılımcısı olma

Kötü amaçlı programlar ve web siteleri ile ilgili bilgilere katkıda bulunarak Gerçek Zamanlı Koruma A ı korumasının geli tirilmesine yardım edebilirsiniz.

Yükleme sırasında Gerçek Zamanlı Koruma A ı'na katılmayı seçebilirsiniz. Varsayılan yükleme ayarlarıyla Gerçek Zamanlı Koruma A ı verilerine katkıda bulunursunuz. Bu ayarları daha sonra ürünün içinde de i tirebilirsiniz.

Gerçek Zamanlı Koruma A ı ayarlarını de i tirmek için a a ıdaki yönergeleri izleyin:

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.  
Açılır menü görüntülenir.
2. **Ortak ayarları aç** seçene ini belirtin.
3. **Di er > Gizlilik**'i seçin.
4. Gerçek Zamanlı Koruma A ı katılımcısı olmak için katılım onay kutusunu i aretleyin.

## Gerçek Zamanlı Koruma A ı ile ilgili sorular

Gerçek Zamanlı Koruma A ı ile ilgili sorular için ileti im bilgileri.

Gerçek Zamanlı Koruma A ı ile ilgili ba ka sorularınız varsa lütfen u adrese ba vurun:

---

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finlandiya

[http://www.f-secure.com/en/web/home\\_global/support/contact](http://www.f-secure.com/en/web/home_global/support/contact)

Bu ilkenin en son sürümü her zaman web sitemizden edinilebilir.

## Aboneli imin geçerli oldu unu nasıl bilebilirim


Abonelik türünüz ve durumunuz **Abonelik durumu** sayfasında gösterilir.

Aboneli inizin süresi dolmak üzereyken veya dolmu sa, kar ılık gelen LaunchPad simgesindeki programın toplam koruma durumu de i ir.

Aboneli inizin geçerlili ini denetlemek için:

1. Ba latma panelinde en sa daki simgeyi sa tıklatın.  
Açılır menü görüntülenir.
2. **Aboneliklerimi görüntüle** seçene ini belirtin.
3. Yüklü programlar için aboneliklerinizle ilgili bilgileri görüntülemek için **Abonelik durumu**'nu seçin.
4. Yüklenebilecek programları görmek için **Yükleme durumu**'nu seçin.

Abonelik durumunuz ve süre sonunuz da programın **statistikler** sayfasında gösterilir. Aboneli inizin süresi dolmu sa, güncelle tirmeleri almaya ve ürünü kullanmaya devam edebilmek için aboneli inizi yenilemeniz gerekir.


 **Not:** Aboneli inizin süresi doldu unda, sistem tepsinizdeki ürün durumu simgesi yanıp söner.

## Eylem merkezi

Eylem merkezi ilgilenmeniz gereken önemli bildirimleri size gösterir.

Aboneli inizin süresi dolduysa veya dolmak üzereyse eylem merkezi sizi bu durumdan haberdar eder. Eylem merkezi mesajının arka plan rengi ve içeri i abonelik türünüze ve durumunuza ba lıdır:


- Abonelik süreniz dolmak üzereyse ve ücretsiz abonelikler mevcutsa mesajın arka plan rengi beyazdır ve bir **Etkinle tir** dü mesi görüntülenir.
- Abonelik süreniz dolmak üzereyse ancak ücretsiz abonelikler mevcut de ilse mesajın arka plan rengi sarıdır ve ekranda **Satın al** ve **Anahtarı gir** dü meleri görüntülenir. Yeni almı oldu unuz bir abonelik varsa **Anahtarı gir** dü mesini tıklatarak size sa lanmı olan anahtarı girebilir ve aboneli inizi etkinle tirebilirsiniz.
- Abonelik süreniz dolduysa ve ücretsiz abonelikler mevcutsa mesajın arka plan rengi kırmızıdır ve bir **Etkinle tir** dü mesi görüntülenir.
- Abonelik süreniz dolduysa ancak ücretsiz abonelikler mevcut de ilse mesajın arka plan rengi kırmızıdır ve ekranda **Satın al** ve **Anahtarı gir** dü meleri görüntülenir. Yeni almı oldu unuz bir abonelik varsa **Anahtarı gir** dü mesini tıklatarak size sa lanmı olan anahtarı girebilir ve aboneli inizi etkinle tirebilirsiniz.

 **Not:** Eylem merkezindeki **Bildirim geçmi ini görüntüle** ba lantısı ürün bildirim mesajlarını içeren bir liste görüntüler, önceki eylem merkezi bildirimleri burada görüntülenmez.

## Aboneli i etkinle tir

Bir ürün için yeni bir abonelik anahtarınız veya kampanya kodunuz varsa, bunu etkinle tirmeniz gerekir.

Aboneli i etkinle tirmek için:

1. Ba latma panelinde en sa daki simgeyi sa tılatın.  
Açılır menü görüntülenir.
2. **Aboneliklerimi görüntüle** seçene ini belirtin.
3. A a ıdakilerden birini seçin:
  - **Aboneli i etkinle tir**'i tılatın.
  - **Kampanya kodunu etkinle tir**'i tılatın.
4. Açılan ileti im kutusunda, yeni abonelik anahtarınızı veya kampanya kodunuzu girin ve **Tamam**'ı tılatın.  
 **pucu:** Abonelik anahtarınızı e-posta yoluyla aldıysanız, anahtarı e-posta iletisinden kopyalayıp bu alana yapı tırabilirsiniz.

Yeni abonelik anahtarını girdikten sonra, yeni abonelik geçerlilik tarihi **Abonelik durumu** sayfasında gösterilir.



## Giri

---

### Konular:

- *Genel koruma durumunuzu görüntüleme*
- *Ürün istatistiklerini görüntüleme*
- *Ürün güncelle tirmelerini i leme*
- *Virüsler ve di er kötü amaçlı yazılımlar nedir*

Bu ürün, bilgisayarınızı virüslere ve di er yazılım uygulamalarına karşı korur.

Ürün, dosyaları tarar, uygulamaları analiz eder ve otomatik olarak güncelle tirme yapar. Sizin hiçbir şey yapmanız gerekmez.

## Genel koruma durumunuzu görüntüleme






**Durum** sayfası, yüklü ürün özelliklerine ve bu ürünlerin geçerli durumuna hızlı bir genel bakış sunar.

**Durum** sayfasını açmak için:

Ana sayfada **Durum**'u tıklayın.

**Durum** sayfası açılır.

Simgeler, programın durumunu ve güvenlik özelliklerini gösterir.

Durum simgesi	Durum adı	Açıklama
	Tamam	Bilgisayarınız korunuyor. Özellik etkinleştirildi ve düzgün çalışıyor.
	Bilgi	Ürün, özelliğin özel durumu hakkında sizi bilgilendirir. Örneğin, özellik güncelleniyor.
	Uyarı	Bilgisayarınız tam olarak korunmuyor. Örneğin, ürün uzun süredir güncelleştirme almadı ya da bir özelliğin durumuyla ilgilenilmesi gerekiyor.
	Hata	Bilgisayarınız korunmuyor. Örneğin, aboneliğinizin süresi doldu ya da önemli bir özellik kapalı.
	Kapalı	Kritik olmayan bir özellik devre dışı bırakıldı.

## Ürün istatistiklerini görüntüleme

Ürünün yüklenmesinden bu yana yaptıkları işlemleri **statistikler** sayfasında görebilirsiniz.

**statistikler** sayfasını açmak için:

Ana sayfada **statistikler**'i tıklayın.

**statistikler** sayfası açılır.

- **Son birkaç güncelleştirme denetimi**, son güncelleştirme saatini gösterir.
- **Virüs ve casus yazılım taraması**, ürünün yüklendikten sonra kaç dosya tarandı ve temizlediğini gösterir.
- **Uygulamalar**, DeepGuard'ın yüklemeyi bu yana kaç programa izin verdiğini veya engellediğini gösterir.
- **Güvenlik duvarı bağlantıları**, yüklemeyi itibaren izin verilen ve engellenen bağlantıların sayısını gösterir.

- **istenmeyen e-posta ve kimlik avı filtreleme**, ürünün geçerli e-posta iletileri ve istenmeyen e-posta iletileri olarak kaç tane e-posta iletilisi algıladı nı gösterir.

## Ürün güncelle tirmelerini i leme


Ürün, korumayı otomatik olarak güncel tutar.

### Veritabanı sürümlerini görüntüleme

**Veritabanı güncelle tirmeleri** sayfasından en son güncelle tirme zamanlarını ve sürüm numaralarını görebilirsiniz.

**Veritabanı güncelle tirmeleri** sayfasını açmak için:

1. Ana sayfada **Ayarlar**'ı tıklatın.

 **Not:** Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. **Di er ayarlar > Veritabanı sürümleri** ö elerini seçin.


**Veritabanı sürümleri** sayfasında, virüs ve casus yazılım tanımları, DeepGuard ve istenmeyen e-posta ve kimlik avı filtrelemenin güncelle tirildi i en son tarih ve sürüm numaraları görüntülenir.

### Cep telefonu geni bant ayarlarını de i tir

Cep telefonu geni bant ba lantı kullanırken güvenlik güncelle tirmelerini kar ıdan yüklemek için seçin.


 **Not:** Bu özellik yalnızca Microsoft Windows 7'de kullanılabilir.

Varsayılan olarak, asıl operatörünüzün a ındayken güvenlik güncelle tirmeleri her zaman kar ıdan yüklenir. Ancak ba ka bir operatörün a ını kullanıyorsanız güncelle tirmeler askıya alınır. Bunun nedeni, örne in farklı ülkelerde ba lantı ücretlerinin operatörlere göre de i ebilmesidir. Ziyaretiniz sırasında bant geni li inden ve maliyetlerden tasarruf etmek için bu ayarı de i tirmeden kullanmak isteyebilirsiniz.

 **Not:** Bu ayar yalnızca cep telefonu geni bant ba lantılar için geçerlidir. Bilgisayarın bir sabit ya da kablosuz a a ba lı oldu u sırada ürün otomatik olarak güncelle tirilir.

Bu ayarı de i tirmek için:

1. Ana sayfada **Ayarlar**'ı tıklatın.

 **Not:** Ayarları de i tirmek için yönetici haklarınız olması gerekir.

2. **Di er ayarlar > Mobil geni bant > Güvenlik güncelle tirmelerini kar ıdan yükle** ö elerini seçin.

3. Cep telefonu ba lantıları için tercih edilen güncelle tirme seçene ini belirleyin:

- **Yalnızca ev operatörümün a ında**

Güncelle tirmeler her zaman asıl operatörünüzün a ındayken kar ıdan yüklenir. Ba ka bir operatörün a ını kullanıyorsanız güncelle tirmeler askıya alınır. Öngörülen maliyetleri göze alarak güvenlik ürününüzü güncel tutmak üzere bu seçene i belirlemeniz önerilir.

- **Hiçbir zaman**

Mobil geni bant kulland ınızda güncelle tirmeler kar ıdan yüklenmez.

- **Her zaman**

Hangi a ı kullanıyor olursanız olun güncelle tirmeler her zaman kar ıdan yüklenir. Maliyetler ne olursa olsun bilgisayarınızın güvenli inin her zaman güncel olmasını istiyorsanız bu seçene i belirleyin.

4. Ev operatörünüzün a ından her çıkı ınızda ayrıca karar vermek istiyorsanız, **Ev operatörümün a ından her çıkı ımda bana sor** seçene ini belirleyin.

### Askıya alınmı güvenlik güncelle tirmeleri

Asıl operatörünüzün a ı dı ında bir cep telefonu geni bant ba lantı kullanırken güvenlik güncelle tirmeleri askıya alınabilir.

Bu durumda, ekranınızın sa alt kö esinde **Askıya Alındı** bildirim duyurusunu görebilirsiniz. Ba lantı fiyatları operatörlere göre de i ebilece inden (örne in farklı ölkelerde) güncelle tirmeler askıya alınır. Ziyaretiniz sırasında bant geni li inin yanı sıra maliyet tasarrufu da yapmak istiyorsanız, bu ayarı de i tirmeden korumayı dü ünebilirsiniz. Ancak yine de ayarları de i tirmek istiyorsanız, **De i tir** ba lantısını tıklatın.



#### Not:

Bu özellik yalnızca Microsoft Windows 7'de kullanılabilir.

## Virüsler ve di er kötü amaçlı yazılımlar nedir

Kötü amaçlı yazılımlar bilgisayarınıza zarar vermek, bilginiz olmadan bilgisayarınızı yasa dı ı amaçlarla kullanmak veya bilgisayarınızdan bilgi çalmak için özel olarak tasarlanmı programlardır.

Kötü amaçlı yazılımlar unları yapabilir:

- Web tarayıcınızın denetimini ele geçirir,
- arama denemelerinizi yeniden yönlendirir,
- istenmeyen reklamlar gösterir,
- ziyaret etti iniz Web sitelerinin kaydını tutar,
- banka bilgileri gibi ki sel bilgilerinizi çalar,
- bilgisayarınızı kullanarak istenmeyen posta gönderir ve
- bilgisayarınızı kullanarak ba ka bilgisayarlara saldırır.

Kötü amaçlı yazılımlar bilgisayarınızın yava lamasına ve kararsız olmasına da neden olabilir Bilgisayarınız aniden çok yava larsa ve sık sık kilitlenirse *kötü amaçlı yazılımlar* oldu undan üphelenebilirsiniz.

## Virüsler

Virüs, genellikle kendini dosyalara ekleyerek sürekli olarak ço altabilen programdır; bilgisayarınıza zarar verebilecek bir eilde di er dosyaların içeri ini de i tirebilir.

Virüs normalde bilginiz olmadan bilgisayarınıza yüklenen bir programdır. Virüs bula tıktan sonra kendisini ço altmaya çalı ır. Virüs unları yapabilir:

- bilgisayarınızın sistem kaynaklarının bir bölümünü kullanır,
- bilgisayarınızdaki dosyaları de i tirebilir veya dosyalara zarar verebilir,
- bilgisayarınızı kullanarak ba ka bilgisayarları etkilemeye çalı abilir,
- bilgisayarınızın yasa dı ı amaçlarla kullanılmasına neden olabilir.

## Casus yazılımlar

Casus yazılımlar ki sel bilgilerinizi toplayan programlardır.

Casus yazılımlar unun gibi ki sel bilgileri toplar:

- Gözattı ınız Internet siteleri,
- bilgisayarınızdaki e-posta adresleri,
- parolalar veya

- kredi kartı numaraları.

Casus yazılımlar neredeyse her zaman açıkça izniniz olmadan kendilerini yükler. Casus yazılımlar yararlı bir programla birlikte ya da yanıltıcı bir açılır pencerede bir seçene i tıklatmanızı sa layarak yüklenebilir.

## Kendini gizleyen yazılımlar

Kendini gizleyen yazılımlar, di er *kötü amaçlı yazılımlar*'ı bulmayı zorla tırır.

Kendini gizleyen yazılımlar, dosyaları ve i lemleri gizler. Bunu genel olarak bilgisayarınızdaki kötü amaçlı etkinli i gizlemek için yaparlar. Kendini gizleyen bir yazılım *kötü amaçlı yazılımlar*'ı gizliyorsa, bilgisayarınızda kötü amaçlı yazılım oldu unu kolay bir ekilde anlayamazsınız.

Bu üründe, özellikle kendini gizleyen yazılımlar için tarama yaparak *kötü amaçlı yazılımlar*'ın kolayca gizlenememesini sa layan bir kendini gizleyen yazılım tarayıcısı vardır.

## Riskli yazılımlar

Riskli yazılımlar bilgisayarınıza zarar vermek amacıyla özel olarak tasarlanmamı lardır, ancak yanlış kullanılırlarsa bilgisayarınıza zarar verebilir.

Riskli yazılımların mutlaka kötü amaçlı yazılım olması gerekmez. Riskli yazılım programları bazı kullanı lı, ancak zararlı olabilecek i levler gerçekte tirir.

Riskli yazılım programlarına örnek olarak unlar gösterilebilir:

- IRC (Internet relay chat) gibi anlık ileti programları,
- bir bilgisayardan di erine Internet üzerinden dosya aktarmaya yönelik programlar,
- veya Internet telefonu programları (VoIP, *Internet Üzerinden Ses Protokolü*).
- VNC gibi Uzaktan Eri im Yazılımları,
- ki ileri korkutarak veya oyuna getirerek sahte güvenlik yazılımları almaya yönlendiren korkutma yazılımları veya
- CD denetimlerini veya kopyalama korumalarını atlamak için tasarlanan yazılımlar.

Programı açık olarak yüklediyseniz ve do ru ekilde kurduysanız, zararlı olma olasılı ı daha azdır.

Riskli yazılım bilginiz dı ında yüklendiyse, büyük olasılıkla kötü amaçlı olarak yüklenmi tir ve kaldırılması gerekir.



## Kötü amaçlı yazılımlara karşı bilgisayarınızı koruma

---

### Konular:

- [Bilgisayarımı nasıl tarayabilirim](#)
- [Dosyalar nasıl taramanın dışında bırakılır](#)
- [Karantina nasıl kullanılır](#)
- [DeepGuard nedir](#)

Virüs ve casus yazılım taraması bilgisayarınızı kişisel bilgileri çalan, bilgisayarınıza zarar veren veya yasadışı amaçlarla kullanan programlara karşı korur.

Varsayılan olarak, tüm kötü amaçlı yazılım türleri hiçbir zarar vermemeleri için bulunur bulunmaz izlenir.

Virüs ve casus yazılım taraması varsayılan olarak yerel sabit sürücülerinizi, çıkarılabilir ortamlarınızı (taşınabilir sürücüler veya CD'ler gibi) ve kartıdan yüklenen içeriği otomatik olarak tarar. E-postalarınızı da otomatik olarak taramak şekilde ayarlayabilirsiniz.

Virüs ve casus yazılım taraması ayrıca bilgisayarınızda *kötü amaçlı yazılım* göstergesi olabilecek de işlevlikleri de izler. Sistem ayarlarında tehlikeli olabilecek de işlevlikler veya önemli sistem işlevlerini de işlevleme denemeleri bulunursa, *kötü amaçlı yazılım* söz konusu olabileceğinden DeepGuard bu programların çalışmasını durdurur.

## Bilgisayarınızı nasıl tarayabilirim

Virüs ve casus yazılım taraması açıkken, bilgisayarınızı zararlı dosyalara karşı otomatik olarak tarar. Aynı zamanda dosyaları elle tarayabilir ve zamanlanan taramalar ayarlayabilirsiniz.

Virüs ve casus yazılım taramasını her zaman açık tutmanızı öneririz. Bilgisayarınızda hiç zararlı dosya olmadıktan emin olmak istediğinizde ya da gerçek zamanlı taramanın dışında bıraktığınız dosyaları taramak isterseniz, dosyalarınızı elle tarayın.

Virüs ve casus yazılım taraması zamanlanan bir tarama ayarlayarak, zararlı dosyaları belirlenen zamanlarda bilgisayarınızdan kaldırır.

## Dosyaları otomatik olarak tarama

Gerçek zamanlı tarama, erişilen tüm dosyaları tarayıp *kötü amaçlı yazılımlar* içeren dosyalara erişimi engelleyerek bilgisayarınızı korur.

Bilgisayarınız bir dosyaya erişmeye çalıştığında, Gerçek zamanlı tarama bilgisayarınızın bu dosyaya erişmesine izin vermeden önce dosyayı kötü amaçlı yazılımlara karşı tarar. Gerçek zamanlı tarama herhangi bir zararlı içerik bulursa, zarar vermemesi için dosyayı karantinaya alır.

### Gerçek zamanlı tarama bilgisayarınızın performansını etkiler mi?

Normalde, çok kısa sürdüğü ve sistem kaynaklarını çok az kullandığı için tarama işlemi fark etmezsiniz. Gerçek zamanlı tarama için kullanılan süre ve sistem kaynakları, dosyanın içeriğine, konumuna ve türüne bağlı olarak değişebilir.

Taranması daha fazla zaman alan dosyalar:

- CD, DVD ve taşınabilir USB sürücüler gibi çıkarılabilir sürücülerdeki dosyalar.
- Sıkı tırlımlı dosyalar, örneğin: .zip dosyaları.

 **Not:** Sıkı tırlımlı dosyalar varsayılan olarak taranmaz.

Gerçek zamanlı tarama şu durumlarda bilgisayarınızı yavaşlatabilir:


- Sistem gereksinimlerini karşılamayan bir bilgisayarınız var ya da
- aynı anda birçok dosyaya erişiyorsunuz; örneğin, taranması gereken birçok dosya içeren bir dizini açıyorsunuz.

## Gerçek zamanlı taramayı açma veya kapatma

*Kötü amaçlı yazılımları* bilgisayarınıza zarar vermeden önce durdurmak için gerçek zamanlı taramayı açık tutun.

Gerçek zamanlı taramayı açmak veya kapatmak için:

1. Ana sayfada **Durum**'u tıklatın.
2. **Bu sayfadaki ayarları değiştir**'i tıklatın.

 **Not:** Güvenlik özelliklerini kapatmak için yönetici haklarınızın olması gerekir.

3. **Virüs ve casus yazılım taraması**'ni açın veya kapatın.
4. **Kapat**'i tıklatın.

## Zararlı dosyaları otomatik olarak izleme

Gerçek zamanlı tarama, size hiçbir şey sormadan zararlı dosyaları otomatik olarak izleyebilir.



Gerçek zamanlı taramanın zararlı dosyaları otomatik olarak izlemesine izin vermek için:

1. Ana sayfada **Ayarlar**'ı tıklayın.



**Not:** Ayarları değiştirmek için yönetici haklarınız olması gerekir.

2. **Bilgisayar Güvenliği > Virüs ve casus yazılım taraması** öğelerini seçin.

3. **Zararlı dosyaları otomatik olarak izle** öğesini seçin.

Zararlı dosyaları otomatik olarak izlemeyi seçmezseniz, gerçek zamanlı tarama zararlı bir dosya bulunduğunda dosyayla ne yapmak istediğini sorar.

### Casus yazılımları izleme

Virüs ve casus yazılım taraması, bilgisayarınıza çalıştırıldığında casus yazılımı hemen engeller.

Bir casus yazılım uygulaması çalıştırılmadan önce, ürün bu uygulamayı engeller ve uygulamayla ne yapmak istediğini karar vermenize izin verir.

Bir casus yazılım bulunduğunda aşağıdaki eylemlerden birini seçin:

Gerçekleştirecek eylem	Casus yazılım için hangi eylemler gerçekleştirilir
Otomatik izle	Bulunan casus yazılıma göre alınacak en iyi önleme ürününün karar vermesine izin verin.
Casus yazılımı karantinaya al	Casus yazılımı, bilgisayarınıza zarar veremeyeceğini karantinaya taşıyın.
Casus yazılımı sil	Tüm casus yazılımla ilgili dosyaları bilgisayarınızdan kaldırın.
Casus yazılımı yalnızca engelle	Casus yazılıma erişimi engelleyin ancak yazılımı bilgisayarınızda bırakın.
Casus yazılımı taramanın dışında bırak	Casus yazılımının çalışmasına izin verin ve yazılımı gelecekteki taramaların dışında bırakın.

### Riskli yazılımları izleme

Virüs ve casus yazılım taraması, riskli yazılımı çalıştırıldığında hemen engeller.

Bir riskli yazılım uygulaması çalıştırılmadan önce, ürün uygulamayı engeller ve uygulamayla ne yapmak istediğini karar vermenize izin verir.

Bir riskli yazılım bulunduğunda aşağıdaki eylemlerden birini seçin:


Gerçekleştirecek eylem	Riskli yazılımlar için hangi eylemler gerçekleştirilir
Riskli yazılımı yalnızca engelle	Riskli yazılıma erişimi engelleyin ancak yazılımı bilgisayarınızda bırakın.
Riskli yazılımı karantinaya al	Riskli yazılımı bilgisayarınıza zarar veremeyeceğini karantinaya taşıyın.
Riskli yazılımı sil	Tüm riskli yazılımla ilgili dosyaları bilgisayarınızdan kaldırın.
Riskli yazılımı taramanın dışında bırak	Riskli yazılımının çalışmasına izin verin ve yazılımı gelecekteki taramaların dışında bırakın.

### İzleme çerezlerini otomatik olarak kaldırma

İzleme çerezlerini kaldırarak, web sitelerinin Internet'te ziyaret ettiğiniz siteleri izlemesini durdurursunuz.

İzleme çerezleri, web sitelerinin ziyaret ettiğiniz web sitelerini kaydetmesine izin veren küçük dosyalardır. İzleme çerezlerini bilgisayarınızdan kaldırmak için bu yönergeleri izleyin.

1. Ana sayfada **Ayarlar**'ı tıklayın.

 **Not:** Ayarları değiştirmek için yönetici haklarınız olması gerekir.

2. **Bilgisayar Güvenliği > Virüs ve casus yazılım taraması** öğelerini seçin.
3. **Özellikler** öğesini seçin.
4. **Tamam**'ı tıklayın.

## Dosyaları elle tarama

Örneğin, bilgisayarınıza harici bir aygıt bağladığınızda, bu aygıtın herhangi bir kötü amaçlı yazılım içerip içermediğinden emin olmak için dosyalarınızı elle tarayabilirsiniz.

### Elle taramayı başlatma

Tüm bilgisayarınızı veya belirli türde *kötü amaçlı yazılımlar*'ı ya da belirli bir konumu tarayabilirsiniz.

Belirli bir türde *kötü amaçlı yazılımlar* olduğundan şüpheleniyorsanız, yalnızca bu tür için tarama gerçekleştirebilirsiniz. Bilgisayarınızdaki belirli bir konumdan şüpheleniyorsanız, yalnızca bu bölümü tarayabilirsiniz. Bu taramalar tüm bilgisayarın taramasından çok daha kısa sürede tamamlanır.

Bilgisayarınızı elle taramayı başlatmak için:

1. Ana sayfada **Tarama**'nın altındaki oku tıklayın.  
Tarama seçenekleri gösterilir.
2. Tarama türünü seçin.  
Elle taramanın, bilgisayarınızı virüslere ve diğer zararlı uygulamalara karşı tarama biçimini iyileştirmek için **Tarama ayarlarını değiştir**'i seçin.
3. **Taranacak öğeleri seçin**'i seçerseniz, taranacak konumu belirleyebileceğiniz bir pencere açılır.  
**Tarama Sihirbazı** açılır.

### Tarama türleri

Tüm bilgisayarınızı veya belirli türde kötü amaçlı yazılımlar'ı ya da belirli bir konumu tarayabilirsiniz.

Aşağıda farklı tarama türleri listelenmiştir:

Tarama türü	Neler taranır	Bu tür ne zaman kullanılır
Virüs ve casus yazılım taraması	Bilgisayarınızın bölümlerinde virüs, casus yazılım ve riskli yazılım taraması	Bu tarama türü tam taramadan çok daha hızlıdır. Sisteminizin yalnızca yüklü program dosyaları bulunan bölümlerini tarar. Bu tarama türü hızlı bir şekilde bilgisayarınızın temiz olup olmadığını denetlemek istiyorsanız önerilir; çünkü bilgisayarınızdaki etkin kötü amaçlı yazılımları etkili bir şekilde bulabilir ve kaldırabilir.
Tam bilgisayar taraması	Bilgisayarınızın tamamında (dahili ve harici sabit sürücüler) virüs, casus yazılım ve riskli yazılım taraması	Bilgisayarınızda kötü amaçlı yazılım veya riskli yazılım olmadığından kesin emin olmak istediğinizde. Bu tarama türü tamamlanması en uzun süren türdür. Hızlı kötü amaçlı yazılım taraması ile sabit sürücü taramasını birleştirir. Bir kendini gizleyen yazılım tarafından gizlenebilecek öğeleri de denetler.
Taranacak öğeleri seçin	Belirli bir dosya, klasör veya sürücüde virüs, casus yazılım ve riskli yazılım taraması	Bilgisayarınızda belirli bir konumda kötü amaçlı yazılımlar olabileceğinden şüpheleniyorsanız; örneğin, konumda öğeler arası dosya paylaşım ağları gibi tehlikeli olabilecek kaynaklardan karıdan yüklenmiş öğeler varsa. Tarama süresi taradığınız hedefin boyutuna göre değişir. Örneğin,

Tarama türü	Neler taranır	Bu tür ne zaman kullanılır
		birkaç küçük dosya içeren bir klasörü tararsanız işlem hızlı bir şekilde tamamlanır.
Kendini gizleyen yazılım taraması	Üçüncü bir işletim sistemi bir güvenlik sorununa neden olabileceği önemli sistem konumları. Gizli dosyaları, klasörleri, sürücülerini veya işlemeleri tarar	Bilgisayarınıza kendini gizleyen bir yazılım yüklediğinden üşheleniyorsanız. Örneğin, yakın zaman önce bilgisayarınız kötü amaçlı yazılım algılandıysa ve bunun bir kendini gizleyen yazılım yüklediğinden emin olmak istiyorsanız.

## Windows Gezgininde tarama

Windows Gezgininde disklerde, klasörlerde ve dosyalarda *virüs*, *casus yazılım* ve *riskli yazılım* taraması yapabilirsiniz.


Bir diski, klasörü veya dosyayı taramak için:

1. Fare ile fareçisini tarama yapmak istediğiniz disk, klasör veya dosya üzerine getirin ve sağ tıklayın.
2. Sağ tıklaytığınızda açılan menüden **Klasörlerde Virüs Taraması Yap** seçeneğini belirleyin. (Seçenek adı, taradığınız işletim sistemi bir disk, klasör veya dosya olmasına bağlı olarak değişir.)  
**Tarama Sihirbazı** penceresi açılır ve tarama başlar.

Bir *virüs* veya *casus yazılım* bulunursa, **Tarama Sihirbazı** temizleme işlemlerinde size yol gösterir.

## Taranacak dosyaları seçme

Elle ve zamanlanan taramalarda *virüsler* ve *casus yazılımlar* için taranmasını istediğiniz dosya türlerini seçebilirsiniz.

1. Ana sayfada **Ayarlar**'ı tıklayın.  
 **Not:** Ayarları değiştirmek için yönetici haklarınız olması gerekir.
2. **Diğer ayarlar > Elle tarama** öğelerini seçin.
3. **Tarama seçenekleri**'nin altında aşağıdaki ayarlar arasından seçim yapın:

### Yalnızca bilinen dosya türlerini tarama


Yürütülebilir dosyalar gibi yalnızca etkilenmesi olası en fazla olan dosya türlerini taramak için. Bu seçeneğin kullanılması ayrıca taramanın hızlanmasını da sağlar. Uzatılara sahip dosyalar taranır: .ani, .asp, .ax, .bat, .bin, .boo, .chm, .cmd, .com, .cpl, .dll, .doc, .dot, .drv, .eml, .exe, .hlp, .hta, .htm, .html, .htt, .inf, .ini, .job, .js, .jse, .lnk, .lsp, .mdb, .mht, .mpp, .mpt, .msg, .ocx, .pdf, .php, .pif, .pot, .ppt, .rtf, .scr, .shs, .swf, .sys, .td0, .vbe, .vbs, .vxd, .wbk, .wma, .wmv, .wmf, .wsc, .wsf, .wsh, .wri, .xls, .xlt, .xml, .zip, .jar, .arj, .lzh, .tar, .tgz, .gz, .cab, .rar, .bz2 ve .hqx.

### Sıkı tırılmış dosyaların işini tarama


Arşiv dosyalarını ve klasörleri taramak için.

### Gelişmiş bulusal yöntem kullan

Yeni ve bilinmeyen kötü amaçlı yazılımları daha iyi bulmak için tarama sırasında tüm kullanılabilir bulusal yöntemleri kullanmak için.

 **Not:** Bu seçeneği belirlerseniz, tarama daha uzun sürer ve daha çok yanlış pozitif sonuç verebilir (zararsız dosyalar üçüncü olarak raporlanabilir).

4. **Tamam**'ı tıklayın.


 **Not:** Dışarıda bırakılan öğeler listesindeki dışarıda bırakılan dosyalar, burada taramalarını seçerseniz bile taranmaz.

## Zararlı dosyalar bulundu unda ne yapmak gerekir

Zararlı dosyalar bulundu unda bunları nasıl işlemek istediğinizi seçin.



Elle tarama sırasında zararlı içerik bulundu unda yapılacak eylemleri seçmek için:


1. Ana sayfada **Ayarlar**'ı tıklayın.

 **Not:** Ayarları değiştirmek için yönetici haklarınız olması gerekir.

2. **Diğer ayarlar > Elle tarama** öğelerini seçin.

3. **Virüs veya casus yazılım bulundu unda** öğesinde, aşağıdaki seçeneklerden birini belirleyin:

Seçenek	Açıklama
<b>Bana sor (varsayılan)</b>	Elle tarama sırasında bulunan her öğe için yapılacak eylemi seçebilirsiniz.
<b>Dosyaları temizle</b>	Ürün, elle tarama sırasında bulunan etkilenen dosyaları otomatik olarak temizlemeye çalışır.  <b>Not:</b> Ürün etkilenen dosyayı temizleyemezse (ağda veya çıkarılabilir sürücülerde bulunmadığı sürece) karantinaya alır, böylece dosya bilgisayara zarar veremez.
<b>Dosyaları karantinaya al</b>	Ürün, elle tarama sırasında bulunan tüm zararlı dosyaları bilgisayara zarar veremeyecekleri karantinaya taşır.
<b>Otomatik olarak sil</b>	Ürün, elle tarama sırasında bulunan tüm zararlı dosyaları siler.
<b>Yalnızca bildir</b>	Ürün, elle tarama sırasında bulunan tüm zararlı dosyaları oldukları gibi bırakır ve tarama raporuna algılamayı kaydeder.  <b>Not:</b> Gerçek zamanlı tarama etkin değilse, bu seçeneği belirlediğinizde kötü amaçlı yazılımlar bilgisayara yine de zarar verebilir.


 **Not:** Zamanlanan tarama sırasında zararlı dosyalar bulundu unda, bu dosyalar otomatik olarak temizlenir.

## Tarama zamanlama

Bilgisayarınızı, virüsleri ve diğer zararlı uygulamaları bilgisayarınızı kullanmadığınızda otomatik olarak tarayıp kaldırmaya ayarlayın ya da bilgisayarınızın temiz olduğundan emin olmak için taramayı düzenli aralıklarla çalışacak şekilde ayarlayın.

Tarama zamanlamak için:

1. Ana sayfada **Ayarlar**'ı tıklayın.

 **Not:** Ayarları değiştirmek için yönetici haklarınız olması gerekir.

2. **Diğer ayarlar > Zamanlanan tarama** öğelerini seçin.

3. **Zamanlanan tarama**'yı açın.

4. Taramanın başlamasını istediğiniz zamanı seçin.

Seçenek	Açıklama
<b>Günlük</b>	Bilgisayarınızı her gün tarayın.
<b>Haftalık</b>	Bilgisayarınızı haftanın seçili günlerinde tarayın. Listedeki günleri seçin.

**Seçenek****Açıklama****Aylık**

Bilgisayarınızı ayın seçili günlerinde tarayın. Günleri seçmek için:

1. **Gün** seçeneklerinden birini seçin.
2. Seçilen günün yanındaki listeden ayın gününü seçin.

5. Seçili günlerde taramayı ne zaman başlatmak istediğinizi seçin.

**Seçenek****Açıklama****Ba langıç saati**

Taramayı belirtilen zamanda başlatın.

**Bilgisayar ı süreyle kullanılmadı ında**

Taramayı bilgisayarınızı belirtilen zaman süresinde kullanmadıktan sonra başlatın.

Zamanlanan tarama bilgisayarınızı tararken elle tarama ayarlarını kullanır, ancak ar ıvleri her zaman tarar ve zararlı dosyaları otomatik olarak temizler.

## E-postaları tarama

E-posta taraması, size gönderilen e-postalarla zararlı dosyalar almanıza karşı sizi korur.

E-postaları virüslere karşı taramak için virüs ve casus yazılım taraması açık olmalıdır.

E-posta taramayı etkinle tirmek için:

1. Ana sayfada **Ayarlar**'ı tıklayın.



**Not:** Ayarları deği tirmek için yönetici haklarınız olması gerekir.

2. **Bilgisayar Güvenli i > Virüs ve casus yazılım taraması** ö elerini seçin.
3. **Zararlı e-posta eklerini kaldır** ö esini seçin.
4. **Tamam**'ı tıklayın.

## E-posta iletileri ve ekler ne zaman taranır

Virüs ve casus yazılım taraması, aldığınız e-postalardaki zararlı içeri i kaldırabilir.

Virüs ve casus yazılım taraması, Microsoft Outlook ve Outlook Express, Microsoft Mail veya Mozilla Thunderbird gibi e-posta programları tarafından alınan zararlı e-posta iletilerini kaldırır. E-posta programınızın POP3 protokolü kullanan posta sunucusundan her e-posta al ında, ifrelenmemiş e-posta iletilerini ve eklerini tarar.

Virüs ve casus yazılım taraması, Hotmail, Yahoo! mail ya da Gmail gibi web tarayıcınızda çalış an e-posta uygulamaları içeren web postasındaki e-posta iletilerini tarayamaz. Zararlı ekleri kaldırmazsanız veya web postası kullansanız bile *virüslere* karşı korunmaya devam edersiniz. E-posta eklerini açtığınızda, gerçek zamanlı tarama, zararlı ekleri zarar vermeden önce kaldırır.



**Not:** Gerçek zamanlı tarama arkadaş larınızı değil, yalnızca bilgisayarınızı korur. Gerçek zamanlı tarama, eki açmadığınız sürece ekli dosyaları taramaz. Bu da, web postası kullanıyorsanız ve ekini açmadan önce bir iletiyi iletirseniz, arkadaş larınıza etkilenen bir e-posta iletilebileceğ iniz anlamına gelir.


## Tarama sonuçlarını görüntüleme

Virüs ve casus yazılım geçmi i, ürünün buldu u tüm zararlı dosyaları görüntüler.

Bazen, ürün zararlı bir ö e bulundu unda seçtiğ iniz eylemi gerçekle tiremez. Örne in, dosyaları temizlemeyi seçerseniz ve bir dosya temizlenemezse, ürün bu dosyayı karantinaya alır. Bu bilgileri virüs ve casus yazılım geçmi inde görüntüleyebilirsiniz.

Geçmi i görüntülemek için:

1. Ana sayfada **Ayarlar**'ı tıklayın.

 **Not:** Ayarları değiştirmek için yönetici haklarınız olması gerekir.

2. **Bilgisayar Güvenliği** > **Virüs ve casus yazılım taraması** öğelerini seçin.


3. **Kaldırma geçmişi görüntüle**'yi tıklayın.

Virüs ve casus yazılım geçmişi ana ekrandaki bilgileri görüntüler:

- zararlı dosyanın bulunduğu tarih ve saat,
- kötü amaçlı yazılımın adı ve bilgisayarınızdaki konumu,
- gerçekleştirilen eylem.

## Dosyalar nasıl taramanın dışında bırakılır

Bazen, bazı dosyaları veya uygulamaları taramanın dışında bırakmak isteyebilirsiniz. Dışarıda bırakılan öğeler, siz onları dışarıda bırakılan öğeler listesinden kaldırıncaya kadar taranmaz.


 **Not:** Dışarıda bırakma listeleri, gerçek zamanlı ve elle tarama için ayrı ayrıdır. Örneğin, bir dosyayı gerçek zamanlı taramanın dışında bırakırsanız, elle taramanın da dışında bırakmadığınız sürece elle tarama sırasında bu dosya taranır.

## Dosya türlerini dışılamak

Dosyaları türlerine göre dışarıda bırakırsanız, belirtilen uzantılara sahip dosyalar zararlı içeriğe karşı taranmaz.

Dışarıda bırakmak istediğiniz dosya türünü eklemek veya çıkarmak için:

1. Ana sayfada **Ayarlar**'ı tıklayın.

 **Not:** Ayarları değiştirmek için yönetici haklarınız olması gerekir.

2. Dosya türünü gerçek zamanlı veya elle taramanın dışında bırakmak isteyip istemediğinizi seçin:

- Dosya türünü gerçek zamanlı taramanın dışında bırakmak için **Bilgisayar Güvenliği** > **Virüs ve casus yazılım taraması** öğelerini seçin.
- Dosya türünü gerçek zamanlı taramanın dışında bırakmak için **Diğer ayarlar** > **Elle tarama** öğelerini seçin.

3. **Dosyaları taramanın dışında bırak**'i tıklayın.

4. Bir dosya türünü dışılamak için:

- Dosya Türleri** sekmesini seçin.
- Uzantılara sahip dosyaları dışılamak**'i seçin.
- Ekle** düğmesinin yanındaki alana, dışılamak istediğiniz dosyaların türünü belirleyen bir dosya uzantısı yazın.  
Uzantısı olmayan dosyaları belirtmek için '.' yazın. Tek bir karakteri belirtmek için '?' joker karakterini, birden çok karakteri belirtmek için '\*' joker karakterini kullanabilirsiniz.  
Örneğin, yürütülebilir dosyaları dışılamak için bu alana exe yazın.
- Ekle** öğesini tıklayın.

5. Virüs taramalarının dışında bırakmak istediğiniz diğer uzantılar için de önceki adımı yineleyin.

6. **Tamam**'i tıklayarak **Tarama Dışında Bırak** iletişim kutusunu kapatın.

7. Yeni ayarları uygulamak için **Tamam**'i tıklayın.


Seçili dosya türleri gelecekteki taramaların dışında bırakılır.

## Konuma göre dosyaları dışarıda bırakma

Dosyaları konuma göre dışarıda bıraktığınızda, belirtilen sürücülerdeki veya klasörlerdeki dosyalar zararlı içeriklere karşı taranmaz.

Dışarıda bırakmak istediğiniz dosya konumlarını eklemek veya kaldırmak için:

1. Ana sayfada **Ayarlar**'ı tıklayın.

 **Not:** Ayarları değiştirmek için yönetici haklarınız olması gerekir.


2. Konumu gerçek zamanlı veya elle taramanın dışarıda bırakmak isteyip istemediğinizi seçin:

- Konumu gerçek zamanlı taramanın dışarıda bırakmak için **Bilgisayar > Virüs ve casus yazılım taraması** öğelerini seçin.
- Konumu elle taramanın dışarıda bırakmak için **Bilgisayar > Elle tarama** öğelerini seçin.

3. **Dosyaları taramanın dışarıda bırak**'ı tıklayın.

4. Bir dosyayı, sürücüyü veya klasörü dışarıda bırakmak için:

- a) **Nesneler** sekmesini seçin.
- b) **Nesneleri dışarıda bırak (dosyalar, klasörler, ...)** öğesini seçin.
- c) **Ekle** öğesini tıklayın.
- d) Virüs taramasının dışarıda bırakmak istediğiniz dosyayı, sürücüyü veya klasörü seçin.

 **Not:** Bazı sürücüler CD, DVD veya ağ sürücülerine gibi taşınabilir sürücüler olabilir. Ağ sürücülerini ve boş taşınabilir sürücüler dışarıda bırakılamaz.

e) **Tamam**'ı tıklayın.

5. Başka dosya, sürücü veya klasörleri virüs taramasının dışarıda bırakmak için önceki adımı yineleyin.

6. **Tamam**'ı tıklayarak **Tarama Dışarıda Bırak** iletişim kutusunu kapatın.

7. Yeni ayarları uygulamak için **Tamam**'ı tıklayın.

Seçili dosyalar, sürücüler veya klasörler gelecekteki taramaların dışarıda bırakılır.

## Dışarıda bırakılan uygulamaları görüntüleme

Taramanın dışarıda bıraktığınız uygulamaları görüntüleyebilir, gelecekte taramak isterseniz bu uygulamaları dışarıda bırakılan öğeler listesinden kaldırabilirsiniz.


Gerçek zamanlı veya elle tarama casus yazılım veya riskli yazılım gibi davranan ancak güvenli olduğunu bildiğiniz bir uygulama algılırsa, ürünün sizi bu yazılımla ilgili daha fazla uyarmaması için yazılımı tarama dışarıda bırakabilirsiniz.

 **Not:** Uygulama virüs ya da diğer kötü amaçlı yazılımlar gibi davranırsa, tarama dışarıda bırakılamaz.

Uygulamaları doğrudan dışarıda bırakamazsınız. Yeni uygulamalar yalnızca tarama sırasında siz bu uygulamaları dışarıda bırakırsanız dışarıda bırakılanlar listesinde görünür.

Tarama dışarıda bırakılan uygulamaları görüntülemek için:

1. Ana sayfada **Ayarlar**'ı tıklayın.

 **Not:** Ayarları değiştirmek için yönetici haklarınız olması gerekir.


2. Gerçek zamanlı veya elle taramanın dışarıda bırakılan uygulamaları görüntülemek isteyip istemediğinizi seçin:

- Gerçek zamanlı taramanın dışarıda bırakılan uygulamaları görüntülemek için **Bilgisayar > Virüs ve casus yazılım taraması** öğelerini seçin.

- Elle taramanın dışında bırakılan uygulamaları görüntülemek için **Bilgisayar > Elle tarama** öğelerini seçin.

3. **Dosyaları taramanın dışında bırak**'ı tıklatın.

4. **Uygulamalar** sekmesini seçin.

 **Not:** Yalnızca casus yazılım ve riskli yazılımlar dışlanabilir, virüsler dışlanamaz.

5. Dışarıda bırakılan uygulamayı yeniden taramak isterseniz:

- a) Taramaya eklemek istediğiniz uygulamayı seçin.
- b) **Kaldır**'ı tıklatın.

6. **Tamam**'ı tıklatarak **Tarama Dışarı Bırak** iletişim kutusunu kapatın.

7. Çıkmak için **Tamam**'ı tıklatın.

## Karantina nasıl kullanılır

Karantina, zararlı olabilecek dosyalar için güvenli bir depodur.

Karantinaya alınan dosyalar yayılamaz veya bilgisayarınıza zarar veremez.

Zarar vermemeleri için *kötü amaçlı yazılımlar*, *casus yazılımlar* ve *riskli yazılımlar*'ı karantinaya alabilirsiniz. Daha sonra gerekirse uygulamaları veya dosyaları karantinadan geri yükleyebilirsiniz.

Karantinaya alınan bir öğe gerekli de ilse onu silebilirsiniz. Karantinadaki bir öğeyi silmek onu bilgisayarınızdan kalıcı olarak kaldırır.


- Genel olarak, karantinaya alınan *kötü amaçlı yazılımlar*'ı silebilirsiniz.
- Çoğu durumda, karantinaya alınan *casus yazılımlar*'ı silebilirsiniz. Karantinaya alınan *casus yazılımlar* yasal bir yazılım programının parçası olabilir ve kaldırıldıklarında asıl program düzgün çalışmayabilir. Programın bilgisayarınızda kalmasını isterseniz, karantinaya alınan *casus yazılımlar*'ı geri yükleyebilirsiniz.
- Karantinaya alınan *riskli yazılım* her bir yazılım programı olabilir. Programı kendiniz yükleyip kurduysanız, karantinadan geri yükleyebilirsiniz. *Riskli yazılım* bilginiz dışında yüklendiyse, büyük olasılıkla kötü amaçlı olarak yüklenmiştir ve kaldırılması gerekir.

## Karantinaya alınan öğeleri görüntüleyin

Karantinaya alınan öğeler hakkında daha fazla bilgi görüntüleyebilirsiniz.

Karantinaya alınan öğeler hakkında daha fazla bilgi görüntülemek için:

1. Ana sayfada **Ayarlar**'ı tıklatın.

 **Not:** Ayarları değiştirmek için yönetici haklarınız olması gerekir.

2. **Bilgisayar Güvenliği > Virüs ve casus yazılım taraması** öğelerini seçin.


3. **Karantinayı görüntüle**'yi tıklatın.

**Karantina** sayfası karantinada depolanan toplam öğe sayısını gösterir.

4. Karantinaya alınan öğeler hakkında daha fazla bilgi görüntülemek için **Ayrıntılar**'ı tıklatın.

Çerçeve zararlı yazılım adına veya dosya yoluna göre sıralayabilirsiniz.

Karantinaya alınmış öğelerin türü, bunların adları ve dosyaların yüklü olduğu yol ile birlikte ilk 100 öğenin listesi görüntülenir.

5. Karantinaya alınmış öğe ile ilgili daha fazla bilgi görüntülemek için, **Durum** sütununda öğenin yanındaki  simgesini tıklatın.



## Karantinaya alınan ö eleri geri yükleme

Karantinaya alınmış ö elerden gereksinim duyduklarınızı geri yükleyebilirsiniz.

Uygulamaları veya dosyaları gerekirse karantinadan geri yükleyebilirsiniz. Hiçbir tehdit oluşturmadıklarından emin olmadıkça ö eleri karantinadan geri yüklemeyin. Geri yüklenen ö eler bilgisayarınızda özgün konumlarına geri taşınırlar.

Karantinaya alınan ö eleri geri yükleme

1. Ana sayfada **Ayarlar**'ı tıklatın.



**Not:** Ayarları değiştirmek için yönetici haklarınız olması gerekir.

2. **Bilgisayar Güvenliği > Virüs ve casus yazılım taraması** ö elerini seçin.
3. **Karantinayı görüntüle**'yi tıklatın.
4. Geri yüklemek istediğiniz karantinaya alınmış ö eleri seçin.
5. **Geri Yükle**'yi tıklatın.

## DeepGuard nedir

DeepGuard dosyaların içeriklerini ve uygulamaların davranışlarını inceler, güvenilmeyen uygulamaları izler.

DeepGuard, bilgisayarınızda değişiklik yapmaya çalışan yeni ve keşfedilmemiş *virüsleri, solucanları* ve diğer zararlı uygulamaları engeller, üpheli uygulamaların Internet'e erişmelerini önler.

DeepGuard, sistemde olası zararlı değişiklikler yapmaya çalışan yeni bir uygulama algıladığında, uygulamanın güvenli bölgede çalışmasına izin verir. Güvenli bölgede, uygulama bilgisayarınıza zarar veremez. DeepGuard uygulamanın yapmaya çalıştığı değişiklikleri inceler ve buna bağlı olarak, uygulamaların *kötü amaçlı yazılım* olma olasılıklarına karar verir. Uygulamanın *kötü amaçlı yazılım* olma olasılığı varsa, DeepGuard bu uygulamayı engeller.

DeepGuard'ın algıladığı olası zararlı sistem değişiklikleri şunlardır:

- sistem ayarları (Windows kayıt defteri) değişiklikleri,
- önemli sistem programlarını (örneğin, bu ürün gibi güvenlik programlarını) devre dışı bırakma denemeleri ve
- önemli sistem dosyalarını düzenleme denemeleri.

## DeepGuard'ı açma veya kapatma

Üpheli uygulamaların bilgisayarınızda olası zararlı sistem değişiklikleri yapmasını önlemek için DeepGuard'ı açık tutun.

Windows XP'niz varsa, DeepGuard'ı açmadan önce Service Pack 2 uygulamasının yüklü olduğundan emin olun.

DeepGuard'ı açmak veya kapatmak için:

1. Ana sayfada **Durum**'u tıklatın.
2. **Bu sayfadaki ayarları değiştir**'i tıklatın.



**Not:** Güvenlik özelliklerini kapatmak için yönetici haklarınızın olması gerekir.


3. **DeepGuard**'ı açın veya kapatın.
4. **Kapat**'i tıklatın.

## DeepGuard'ın engellediği uygulamalara izin verme

DeepGuard'ın hangi uygulamalara izin verdiğini ve hangilerini engellediğini denetleyebilirsiniz.

Bazen, bir uygulamayı kullanmak isterseniz ve güvenli olduğunu bilseniz bile, DeepGuard güvenli uygulamanın çalışmasını engelleyebilir. Bu durum, uygulama zararlı olabilecek sistemdeki işlevleri yapmaya çalıştığı için olabilir. Ayrıca, DeepGuard açılır penceresi görüntülendiğinde uygulamayı yanlışlıkla siz de engellemi olabilirsiniz.

DeepGuard'ın engellediği uygulamaya izin vermek için:


1. Ana sayfada **Araçlar**'ı tıklayın.
2. **Uygulamalar**'ı tıklayın.  
**Engellenen uygulamalar** listesi görüntülenir.
3. İzin vermek istediğiniz uygulamayı bulun.  
 **Not:** Listeyi sıralamak için sütun başlıklarını tıklatabilirsiniz. Örneğin, listeyi izin verilen ve reddedilen programlar olarak gruplar halinde sıralamak için **İzinler** sütununu tıklayın.
4. **İzinler** sütununda **İzin Ver**'i seçin.
5. **Kapat**'ı tıklayın.

DeepGuard uygulamanın sistemdeki işlevleri yapmasına yeniden izin verir.

## DeepGuard'ı uyumluluk modunda kullanma

Maksimum koruma için, DeepGuard çalışan programları geçici olarak devre dışı bırakır. Bazı programlar, bozulup bozulmadıkları veya devre dışı bırakılıp bırakılmadıklarını ve bu özellikle uyumlu olup olmadıklarını denetler. Örneğin, hile önleme araçları bulunan çevrimiçi oyunlar, çalışırken herhangi bir şekilde devre dışı bırakılıp bırakılmadıklarını denetler. Bu gibi durumlarda, uyumluluk modunu açabilirsiniz.

Uyumluluk modunu açmak için:

1. Ana sayfada **Ayarlar**'ı tıklayın.  
 **Not:** Ayarları devre dışı bırakmak için yönetici haklarınız olması gerekir.
2. **Bilgisayar Güvenliği** > **DeepGuard** öğelerini seçin.
3. **Uyumluluk modunu kullan** öğesini seçin.
4. **Tamam**'ı tıklayın.

## Üşüpheli davranış uyarılarıyla ne yapmak gerekir

DeepGuard güvenilmeyen uygulamaları izler. Engellenen bir uygulama Internet'e erişmeyi denerse, sisteminizde de işlev yapmaya çalışırsa ya da üşüpheli davranırsa, DeepGuard bu uygulamayı engeller.

DeepGuard ayarlarında **Üşüpheli davranış hakkında beni uyar** seçeneğini belirlediğinizde, DeepGuard, olası zararlı bir uygulama algıladığında veya tanınmayan bir uygulamayı çalıştırdığınızda sizi uyarır.

DeepGuard'ın engellediği bir uygulamayla ne yapmak istediğinizde karar vermek için:

1. Programla ilgili daha fazla bilgi görüntülemek için **Ayrıntılar**'ı tıklayın.  
Ayrıntılar bölümünde bunları görürsünüz:
  - uygulamanın konumu,
  - Gerçek Zamanlı Koruma A'ında uygulamanın tanınırlığı,
  - uygulamanın ne kadar yaygın olduğunu.
2. DeepGuard'ın engellediği uygulamaya güvenip güvenmediğinize karar verin:

- Uygulamayı engellemek istemiyorsanız **Uygulamaya güveniyorum. Devam etmesine izin ver.** seçeneğini belirleyin.

bu durumlarda uygulamanın güvenli olması olasıdır:

- DeepGuard, sizin yaptığınız bir eylem sonucu uygulamayı engelledi,
  - uygulamayı biliyorsunuz ya da
  - uygulamayı güvenilir bir kaynaktan edindiniz.
- Uygulamanın engellenmesini istiyorsanız **Uygulamaya güvenmiyorum. Engelli kalmasını sağla.** seçeneğini belirleyin.

Uygulama bu durumlarda güvenli olmayabilir:

- Uygulama yaygın değil,
- uygulama tanınmıyor ya da
- uygulamayı bilmiyorsunuz.

**3. Şüpheli bir uygulamayı analize göndermek istiyorsanız:**

- a) **Uygulamayı F-Secure'a bildir**'i tıklayın.

Ürün, gönderme koşullarını görüntüler.

- b) Koşulları kabul ediyorsanız ve örneğin göndermek istiyorsanız **Kabul Et**'i tıklayın.

bu durumlarda bir örnek göndermenizi öneririz:

- DeepGuard güvenli oldu diye bildiren bir uygulamayı engelledi ya da
- uygulamanın *kötü amaçlı yazılım* olabileceğinden şüphelendiniz.

